基于多类型数据包的 IPv6 防火墙防护能力评测方法 *

辜苛峻 [1,2]，张连成 [1,2†]，郭　毅 [1,2]，孔亚洲 [1,2]，王振兴 [1,2]

(1. 信息工程大学，郑州 450001; 2. 数学工程与先进计算国家重点实验室，郑州 450001)

摘　要：为测试 IPv6 防火墙对潜在 IPv6 网络威胁的防护能力，研究 IPv6 防火墙防护能力评测方法。通过对 IPv6 协议的研究，本文构造了针对 ICMPv6、单一扩展报头、多扩展报头、分片、地址范围的五类存在安全隐患的测试数据包，构建了 C/S 架构的防火墙测试框架，并基于框架和测试数据包构建了用于各类测试的独立测试模块，搭建了可用于测试有状态防火墙的测试环境，并提供了相应的测试方法。利用本文所提出的方法，对思科 ASA5505 防火墙进行了测试，发现了它的一些优点与不足。

关键词：IPv6；防火墙；防护能力

中图分类号：TP393.08　　doi: 10.3969/j.issn.1001-3695.2018.01.0043

IPv6 firewall defensive capability testing method based on varied packets

Gu Kejun[1,2], Zhang Liancheng[1,2†], Guo Yi[1,2], Kong Yazhou[1,2], Wang Zhenxing[1,2]

(1. *Information Engineering University*, *Zhengzhou* 450001, *China*; 2. *State Key Laboratory of Mathematical Engineering & Advanced Computing*, *Zhengzhou* 450001, *China*)

Abstract: In order to test the defensive capability of IPv6 firewall to against potential IPv6 network threats, this paper studied IPv6 firewall defensive capability testing technology. Through the research of IPv6 protocol, this paper constructed five kinds of test packets with security risks, such as ICMPv6, single extended header, multi-extension header, fragmentation and address scopes, proposed a firewall testing framework with C/S architecture, built independent test modules for every kind of testing based the framework and test packets, set up test environments that can be used to test stateful firewalls, and provided appropriate test methods. Using the method, this paper tested a Cisco ASA5505 firewall and found its advantages and disadvantages.

Key words: IPv6; firewall; defensive capability

0　引言

随着物联网的蓬勃发展，接入互联网的设备数量不断增加。而在 2011 年 2 月 3 日，号码资源组织（Number Resource Organization，NRO）宣布全球互联网数字分配机构（Internet Assigned Numbers Authority，IANA）已经将 IPv4 地址库剩余的 5 个 A 级地址平均分配给包括亚太互联网络信息中心（Asia-Pacific Network Information Center，APNIC）在内的五个地区性互联网注册管理机构（Regional Internet Registry，RIR）[1]。APNIC 给出了全球五个 RIR 近几年剩余的 IPv4 地址块数量随时间变化图及对今后变化趋势的预测[2]，如图 1 所示。可以看出各 RIR 都已经将最后的/8 地址块分出，且预计到 2021 年所有地区的 IPv4 地址将全部分完。而 IPv6 网络巨大的地址空间能完美解决当前地址不足的尴尬局面。除此之外，IPv6 在安全性方面较 IPv4 也有了较大改观，能进行更准确的源地址认证和路由验证等，因而在部分欧美国家得到了广泛的推广和使用。2017 年 11 月 26 日，中共中央办公厅、国务院办公厅印发了《推进互联网协议第六版（IPv6）规模部署行动计划》，这标志着 IPv6 网络也即将在我国进行规模化部署。

随着互联网的发展，网络安全事件层出不穷，网络安全已成为人们最为关注的焦点之一。防火墙作为最基本的网络安全设备，为内网安全提供了重要保障。随着 IPv6 网络的规模化部署，IPv6 防火墙将为 IPv6 网络安全提供坚强保障。因此，针对 IPv6 防火墙防护能力的测试变得尤为重要。

IPv6 防火墙的防护能力主要体现在两个方面：a）防火墙默认配置下能否阻止可能导致安全问题的数据包通过防火墙；b）防火墙能否通过配置相应规则阻止 a）中不能阻止的数据包通过防火墙。

本文为测试 IPv6 防火墙的防护能力，构造了一系列存在安全隐患的 IPv6 测试数据包，构建了一个 IPv6 防火墙测试框架，

收稿日期：2018-01-29；**修回日期：**2018-03-09　**基金项目：**国家自然科学基金资助项目（61402526、61402525）

作者简介：辜苛峻（1993-），男，四川荣县人，硕士研究生，主要研究方向为 IPv6 网络安全；张连成（1982-），男（通信作者），讲师，博士，主要研究方向为信息安全、流量分析（liancheng17@gmail.com）；郭毅（1984-），男，讲师，博士，主要研究方向为路由安全、复杂网络；孔亚洲（1989-），男，博士研究生，主要研究方向为信息安全、IPv6 网络安全；王振兴（1959-），男，教授，博导，主要研究方向为信息安全、网络安全.

搭建了可用于测试有状态防火墙与无状态防火墙的通用测试环境。对思科 ASA 5505 防火墙进行了测试，对测试结果进行了分析，并提出下一步研究方向。

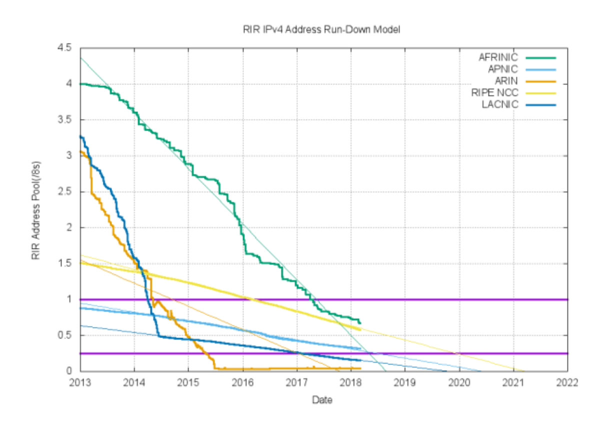


图 1　RIR 剩余 IPv4 地址数量及预测

1　防火墙防护能力评测技术分析

当前针对防火墙测试的研究主要用于黑盒测试，通过发送各种数据包测试其能否通过防火墙以求还原防火墙的配置规则。根据其测试机制可以分为两类：a）基于错误数据包的测试，利用发送错误数据包，使其通过防火墙后在后续路由器上产生因特网控制报文协议（Internet control message protocol，ICMP）差错报文，通过测试端是否收到该 ICMP 差错报文来判定该数据包能否通过防火墙；b）基于端口扫描的测试，利用发送传输控制协议（transmission control protocol，TCP）报文或者用户数据报协议（user datagram protocol，UDP）报文，通过接收端的回应以判断其能否通过防火墙。

David 等人[3]提出的 Firewalking 理论，其使用类似于路由跟踪的 IP 数据包分析方法来测定一个特殊的数据包是否能够从测试者的主机传送到位于数据包过滤设备后的目标主机，以测试防火墙的特定防护规则是否生效。它主要是利用了 IP 数据报报头的生存时间（time to live，TTL）字段，使防火墙后的路由器由于收到 TTL 耗尽的数据包而返回 ICMP 数据报，从而判定特定的探测包能否通过防火墙，以测试防火墙的可靠性。

基于同步信号（synchronous，SYN）扫描的防火墙测试方法，该方法利用向位于防火墙之后的主机发送含特定端口号的 TCP-SYN 请求包，若测试端收到回复，则说明该端口号可以通过防火墙，以测试防火墙的端口防护能力。

Firewalking 是基于网络层的技术，能广泛应用于对应用层、IP 层的测试，但不能用于对 ICMP 差错报文的测试；而且该技术还需要一个额外的路由器进行配合，提高了测试成本，而其作为判定依据的 ICMP 数据包也极有可能被防火墙拦截，导致测试结果不可靠。基于 SYN 扫描的防火墙测试技术只能用于针对应用层的测试，不能针对 ICMP 和 IP 层进行测试，且新一代防火墙大多带有防 SYN 扫描功能，也可能导致测试结果不准确。

当前对防火墙测试技术的研究主要针对 IPv4 防火墙，少有针对 IPv6 防火墙的测试技术研究。IPv6 协议中 ICMPv6 比 ICMP 增加了更多的功能，以及 IPv6 除了固定的报头外还有不限数量的扩展报头。而且本文主要目的在于测试 IPv6 防火墙的防护能力，除了需要获取数据包能否通过防火墙的信息外，还需构造具有 IPv6 特色的存在安全隐患的测试数据包。

2　多类型测试数据包的构造

通过对 IPv6 协议的研究、对 IPv6 网络安全的研究，针对 IPv6 网络的特点，构造具有安全隐患的 IPv6 防火墙测试数据包，以测试防火墙对各类存在安全隐患测试包的防护能力。根据测试数据包的类型，将其分为针对 ICMPv6 的测试、针对单扩展报头的测试、针对多扩展报头的测试、针对分片攻击的测试以及针对地址作用范围的测试。

2.1　针对 ICMPv6 的测试数据包构造

ICMPv6 报文主要分为错误类报文和信息类报文两类。其具有差错报告、网络诊断、邻节点发现和多播实现等功能。RFC 4890 中对防火墙拦截 ICMPv6 报文提出了建议，本文据此将 ICMPv6 报文分为三类：

a）不应该被防火墙拦截的。如表 1 所示，其中前四项为 IPv6 网络中通信建立和维护所必需的错误消息，最后一项是 Teredo 隧道中必不可少的回送请求/应答消息[4~6]。在 IPv4 网络中，防火墙拦截回送请求消息，以降低对受保护网络的扫描攻击风险；而 IPv6 网络中，一个子网拥有海量地址空间，降低了其受到扫描攻击的概率，因而在 IPv6 网络中防火墙不应该拦截回送请求/应答消息。

b）应该被防火墙拦截的。如表 2 所示，如只应该作用于本地链路的协议（本地链路多播协议、邻居发现协议、安全邻居发现（SEcure neighbor discovery protocol，SEND）路径认证通知协议及多播路由器发现协议）和一些未使用的保留类型。

c）其余为可以被防火墙拦截的。这类消息能否通过防火墙对整个网络不会造成大的影响，因而在需要的时候可以通过防火墙设置允许其通过防火墙。

表 1　应该通过防火墙的 ICMPv6 报文

ICMPv6 类型	描述
1	目标不可达
2	数据包过大
3, Code 0	TTL 为 0
4, Code 1,2	下一报头无法识别/无法识别的 IPv6 选项
128, 129	回送请求/应答

表 2　应该被防火墙拦截的 ICMPv6 报文

ICMPv6 类型	描述
100, 101, 200, 201	保留用于实验
130-132, 143	本地链路多播协议
133-137, 141, 142	邻居发现协议
148, 149	SEND 路径认证通知协议
151-153	多播路由器发现协议
127, 255	保留用于扩展

ICMPv6 报文中类型字段确定了 ICMPv6 报文的类型，对于一些类型的报文，代码字段对其进行了更精确的分类。本文利用 Scapy 库，生成上述前两类 ICMPv6 测试包，对防火墙进行测试。

2.2　针对扩展报头的测试数据包构造

IPv6 报头和扩展报头取代了 IPv4 报头和可选项，新的扩展报头格式使 IPv6 更适应不同的需求。与 IPv4 报头中的可选项不同，IPv6 扩展报头没有大小限制，可以容纳所有 IPv6 通信所需要的扩展数据。本文主要利用逐跳选项扩展报头、目标选项扩展报头及路由扩展报头对防火墙进行测试，分为单扩展报头测试和多扩展报头测试。

2.2.1 单扩展报头

路由扩展报头中包含路由类型及段剩余，用于表示特定路由类型和还需访问的中间目标数。当路由类型为 0 时，表示采用自由源路由。由于自由源路由允许多个相同地址存在于同一个路由扩展报文中，发送方可让数据包在两个特定路由器之间来回转发以实施拒绝服务攻击来消耗网络资源。当剩余段为 0 时，可以忽略该扩展报头。而移动 IPv6 需要路由类型为 2、段剩余为 1 的路由扩展报头支持[7,8]。因此，防火墙应该拦截路由类型为 0 且段剩余不为 0 的数据包，当不使用移动 IPv6 时甚至可以直接拦截掉所有含路由扩展报头的数据包。因此利用 Scapy，生成含如表 3 所示的三种路由扩展报头的数据包以供测试。

表 3　针对路由报头的测试数据包

路由报头类型	段剩余	防火墙的预期操作
0	1	拦截
0	0	通过
2	1	通过

表 4　针对目标选项报头与逐跳选项报头的测试数据包

选项组合	防火墙的预期操作
无	通过
Jumbo, PadN, Jumbo	拦截
路由警告, Pad1, 路由警告	拦截
快速开始，隧道封装限制, PadN, 快速开始	拦截
RPL, PadN, RPL	拦截

目标选项扩展报头与逐跳选项扩展报头拥有类似的选项结构，根据 RFC 4942，除 Pad1 与 PadN 外，其余选项类型最多只能出现一次，故构造了如表 4 所示的选项组合，并分别加入目标选项扩展报头与逐跳选项扩展报头，以对防火墙进行测试。

2.2.2 多扩展报头

IPv6 协议中没有对扩展报头的长度和数量进行限制，但 RFC 8200 中对其提出了三项建议[12]：a）目标选项报头最多出现两次（第一次在路由报头之前，第二次在上层协议之前）；b）其余选项最多出现一次；c）逐跳选项报头必须紧跟 IPv6 基本报头。同时它也提出 IPv6 节点应该支持任意顺序任意出现次数的扩展报头，故构造了如表 5 所示的扩展报头组合，以测试防火墙对扩展报头顺序数量有无严格要求。

表 5　针对多扩展报头的测试数据包

扩展报头组合	防火墙的预期操作
目标选项，逐跳选项	拦截
逐跳选项，逐跳选项	拦截
目标选项，路由报头，目标选项	通过
逐跳选项，目标选项，路由选项，逐跳选项	拦截

2.3　针对分片攻击的测试数据包构造

在 2012 年 BlackHat 大会上， Atlasis[13]提出了基于分片攻击 IPv6 的方法，其中主要分为重叠分片攻击与超小分片攻击。重叠分片攻击如图 2 所示。利用重组时后续分片内容覆盖了先前分片的部分内容，以达到修改分片内容的目的。根据结果的不同，可分为对端口号进行修改的重叠分片攻击与对载荷进行修改的重叠分片攻击。超小分片攻击指在扩展报头较多的情况下，第一个分片中不包含上层协议头，而试图利用防火墙对第二个分片过滤不严格，使非法流量穿透防火墙的攻击方法，如图 3 所示。通过构造如表 6 所示的数据包来对防火墙进行测试。

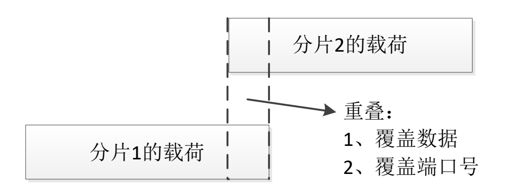


图 2　重叠分片攻击

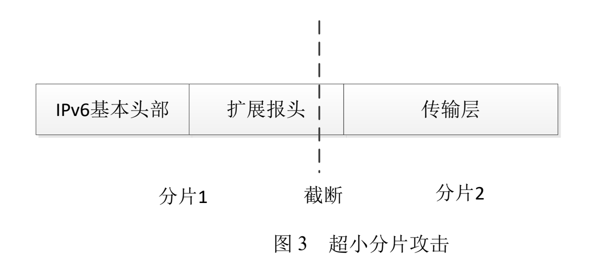


图 3　超小分片攻击

表 6　针对分片攻击的测试数据包

分片类型	防火墙的预期操作
不重叠的分片包	通过
覆盖上层协议头	拦截
覆盖数据部分	拦截
第二个分片携带防火墙允许的端口号	通过
第二个分片携带防火墙禁止的端口号	拦截

2.4　针对地址作用范围的测试数据包构造

多播地址不能作为源地址，而本地链路地址作用域为整个本地链路。如表 7 所示，本文通过构造以多播地址和本地链路地址为源地址的 IPv6 数据包，以测试防火墙的相关功能。

表 7　针对地址作用范围的测试数据包

源地址类型	防火墙的预期操作
多播地址（FF00::/32-FFFF::/32）	拦截
本地链路地址（FE80::/16-FEBF::/16）	拦截

3　IPv6 防火墙测试框架

本文利用 Python 与 Scapy 开发了一个客户/服务器（client/server，C/S）架构的 IPv6 防火墙测试框架，该框架利用 TCP 连接实现测试的同步与测试结果的回传。针对上文提到的五种测试，分别构建了相互独立的测试模块，使每种测试可以独立运行。每一个独立的测试模块分为客户端部分与服务端部分，客户端部分负责则测试包的生成与发送，服务端部分负责测试包的接收与处理。其流程如图 4 所示。

本文采用了如图 5 所示的拓扑图搭建实际测试环境进行测试。对于一般测试，只需客户端、防火墙及服务端即可，而对于针对 ICMPv6 错误类报文的测试而言，则需要如图 5 所示的拓扑。由于 ICMPv6 错误类报文是针对已发出的数据包在传输过程中产生错误而向源发送端发送的错误说明报文，对于有状态的防火墙，若收到 ICMPv6 错误报文且其所携带的原错误报文不是从自己方发出的，会直接将其丢弃，但并不能说明其会拦截正确的 ICMPv6 差错报文。利用如该拓扑图所示的环境，在服务端构造数据包发往辅助端，配置辅助防火墙静默丢弃该数据包。将客户端伪装为辅助防火墙，生成源 MAC 地址和源 IPv6 地址为辅助防火墙对应地址的 ICMPv6 错误消息，并将服务端构造的数据包放入 ICMPv6 消息的数据部分，发往服务端，以测试防火墙对正确的 ICMPv6 差错报文的过滤规则。

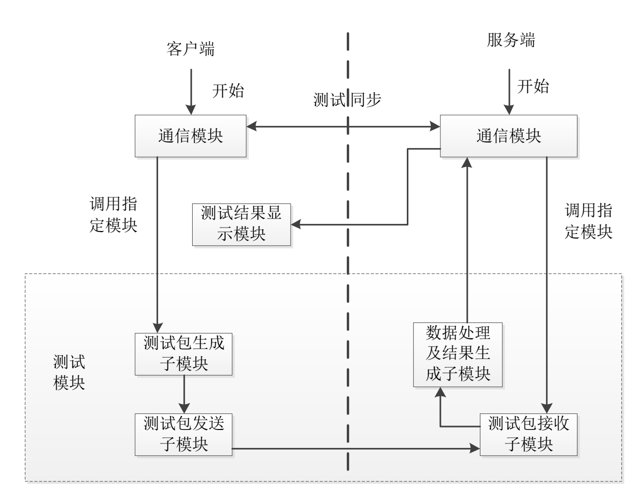


图 4　测试流程

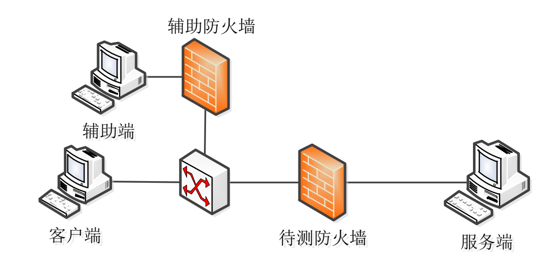
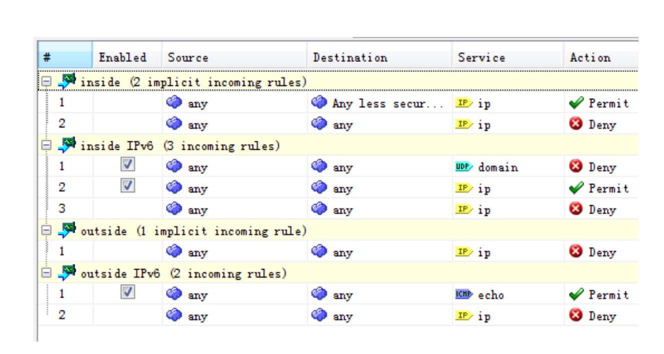


图 5　测试环境拓扑图

4　实验结果与分析

利用上述防火墙测试框架、测试环境及五种测试模块，对思科 ASA 5505 防火墙进行了测试，验证了本文所提出的防火墙测试方法的实用性，检测出了被测设备的若干问题。

思科 ASA 5505 防火墙是一款市场上常见的 ASA（adaptive security appliance）系列防火墙，支持 IPv4&IPv6 双栈接入，常用于企业或分支机构。本文采用的 ASA 5505 防火墙的 ASA 系统版本为 8.2(5)，其设备管理版本为 6.4(5)。将防火墙规则配置为允许所有流量从客户端发往服务端，以测试其内在默认规则是否满足 RFC 标准，是否存在安全隐患。若存在安全问题，则考虑其能否通过配置防火墙相关规则进行避免。配置防火墙拦截 UPD/53 流量，用于测试防火墙针对分片攻击的防护能力。配置防火墙允许从服务端向辅助端发送回送请求消息，用于测试防火墙对正确的 ICMPv6 差错报文的过滤规则。防火墙配置如图 6 所示。



#	Enabled	Source	Destination	Service	Action
inside (2 implicit incoming rules)					
1		any	Any less secur...	ip	Permit
2		any	any	ip	Deny
inside IPv6 (3 incoming rules)					
1	✓	any	any	domain	Deny
2	✓	any	any	ip	Permit
3		any	any	ip	Deny
outside (1 implicit incoming rule)					
1		any	any	ip	Deny
outside IPv6 (2 incoming rules)					
1	✓	any	any	echo	Permit
2		any	any	ip	Deny

图 6　ASA5505 防火墙初始配置

首先使用客户端直接向服务端发送测试包的一般测试方法针对 ICMPv6 进行测试，其部分结果如图 7 所示。其中红色部分表示与预期结果不符。从图 7 中可以看出，防火墙将 ICMPv6 错误报文全部丢弃，故考虑该防火墙为有状态防火墙，利用本章提出的针对有状态防火墙的测试方法进行测试。针对各模块的整体测试结果如图 8 所示。其中红色表示进行该模块测试时存在与预期不符的结果，绿色表示该模块中的所有测试均符合预期结果。将 ICMPv6 测试模块的详细结果整理为如表 8 所示。可以看出采用本章提出的测试方法后，ICMPv6 差错报文的测试结果均与预期相符。这说明了 ASA5505 防火墙的确是一个有状态防火墙，其能记录通过自己发出的数据包，以拦截伪造的 ICMPv6 差错报文，而不会拦截通信过程中正常产生的 ICMPv6 差错报文，这样可以避免非法流量穿透防火墙，且不影响 IPv6 网络的正常运行。对于测试结果中 ICMPv6 类型为 133-153 的 ICMPv6 报文，其作用域为本地链路，不应该被防火墙转发到外网，而测试结果显示其穿过防火墙到达了服务端。由于在 IPv6 网络中，针对本地链路的攻击方法众多，如基于邻居发现协议的地址探测、中间人攻击和拒绝服务（denial of service，DoS）攻击[14,15]，若防火墙不拦截该类协议的数据包，使其能远程发往目标网络，则可能使原本实施条件苛刻的本地链路攻击方法升级为远程攻击方法。对于该类报文，可以配置防火墙，使其拦截地址不是在本网络范围中的该类报文。对于 ICMPv6 类型为 200, 201, 255 的报文，由于该类型为保留类型，若使该类报文出现在网络中可能导致一些未知的错误，可以直接配置防火墙规则将该类报文丢弃。

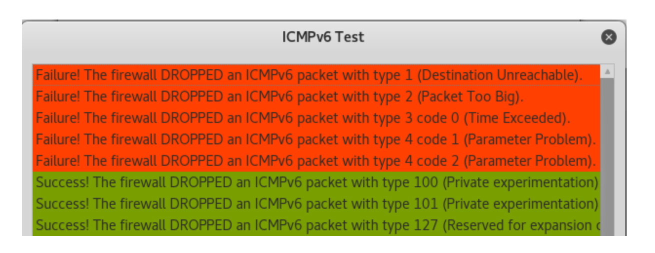


图 7 一般测试方法下 ICMPv6 部分测试结果

针对单扩展报头的测试，将其详细测试结果整理为如表 9 所示。对于路由报头，由于担心被滥用导致任意链路的 DoS 攻击，ASA5505 完全禁止了含路由报头的数据包通过防火墙。由于部署移动 IPv6 需要类型为 2，段剩余为 1 的路由报头支持，所以 ASA5505 不能用于部署移动 IPv6。测试结果表明目标选项报头和逐跳选项报头携带的任意选项组合均能通过防火墙，表明 ASA5505 防火墙并不会对其选项进行检查。而 ASA5505 的防火墙配置中也没有如此细粒度的规则，故 ASA5505 对目标选项报头和逐跳选项报头的选项字段不具备检查能力。由于这两种扩展报头要求中间节点或目标节点对其进行处理，若对其选项不作要求，可能被他人利用，对传输路径上的中间节点或目标节点进行 DoS 攻击。由于扩展报头紧跟着 IPv6 基本报头，若数据包含有扩展报头，则基本包头中的网络层协议字段为扩展报头协议号。其中逐跳选项报头协议号为 0，目标选项报头协议号为 60。尝试在 ASA5505 中配置相应过滤规则，测试 ASA5505 对扩展报头的拦截能力。其配置结果如图 9 所示。不能将网络层协议号设为 0，故只设置 ASA5505 防火墙拦截网络层协议号为 60 的数据包。运行测试，其结果与之前相同，说明 ASA5505 防火墙不能针对扩展报头种类进行人为拦截。

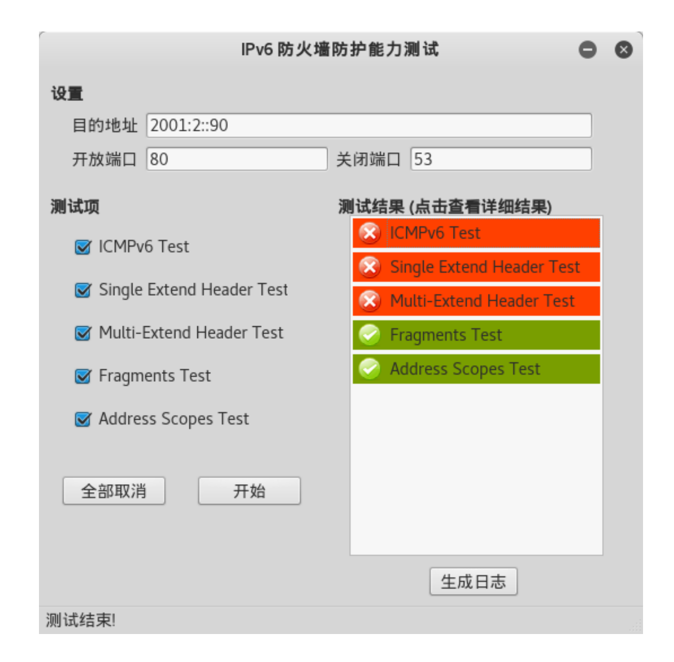


图 8 多模块测试结果

表 8 ICMPv6 测试模块详细结果

ICMPv6 类型	测试结果	是否相符预期
1	通过	是
2	通过	是
3, Code 0	通过	是
4, Code 1,2	通过	是
100, 101, 127	拦截	是
128, 129	通过	是
130-132	拦截	是
133-137, 141, 142, 143	通过	否
148, 149	通过	否
151-153	通过	否
200, 201, 255	通过	否

表 9 单扩展报头测试模块详细结果

扩展报头类型	选 项 组 合	测试结果	是否相符预期
	类型为 0，段剩余为 1	拦截	是
路由扩展报头	类型为 0，段剩余为 0	拦截	否
	类型为 2，段剩余为 1	拦截	否
逐跳扩展报头	无	通过	是
/目的扩展报	Jumbo, PadN, Jumbo	通过	否

头	路由警告，Pad1，路由警告	通过	否
	快速开始，隧道封装限制,PadN，快速开始	通过	否
	RPL, PadN, RPL	通过	否

#	Enabled	Source	Destination	Service	Action
inside (2 implicit incoming rules)					
1		any	Any less secur...	ip	Permit
2		any	any	ip	Deny
inside IPv6 (4 incoming rules)					
1	☑	any	any	DSTOPT 60	Permit
2	☑	any	any	domain	Deny
3	☑	any	any	ip	Permit
4		any	any	ip	Deny
outside (1 implicit incoming rule)					
1		any	any	ip	Deny
outside IPv6 (2 incoming rules)					
1	☑	any	any	echo	Permit
2		any	any	ip	Deny

图 9　针对目的扩展报头的防火墙规则

针对多扩展报头的测试，将其详细测试结果整理为如表 10 所示。可以看出，防火墙对扩展报头顺序数量并没有要求，都能通过防火墙。该特性可能被人利用，通过构造大量逐跳选项报头，降低整个通信路径上通信质量[16]；通过构造大量目标选项报头，对目标节点实施 DoS 攻击[17]；通过大量构造各类扩展报头，利用扩展报头携带通信数据规避防火墙的检查[18]。

表 10　多扩展报头测试模块详细结果

扩展报头组合	测试结果	是否相符预期
目标选项，逐跳选项	通过	否
逐跳选项，逐跳选项	通过	否
目标选项，路由报头，目标选项	通过	是
逐跳选项，目标选项，路由选项，逐跳选项	通过	否

如图 8 所示，针对分片和地址范围的测试结果均符合预期。从分片测试的结果也可以证明该防火墙为有状态防火墙，它能记录之前通过的分片，并据此对后续分片进行检测，而有效避免他人利用分片数据包规避对通信内容和端口的检查。从地址范围测试的结果可以看出，ASA5505 防火墙能丢弃源地址为多播地址及本地链路地址的数据包，这可以有效避免从外网发起的针对内网本地链路的反射攻击。

5　结束语

本文构造了五种存在安全隐患的测试数据包，利用 Python 和 Scapy 构建了 C/S 架构的测试框架，并基于框架和测试数据包构建了用于各类测试的独立测试模块。通过对 ICMPv6 差错报文产生机制的分析，搭建了可用于测试有状态防火墙的测试环境，并提供了相应的测试方法。利用本文所提出的方法，对思科 ASA 5505 防火墙进行了测试。经测试发现 ASA5505 是一个有状态防火墙，对基于 ICMPv6 差错报文的防火墙穿透和基于分片的防火墙穿透有很好的防范效果。对于作用域为本地链路的本地链路地址和多播地址，ASA5505 能将含有此类地址的数据包丢弃，有效避免从外网发起的针对内网本地链路的反射攻击。ASA5505 默认配置下不能将邻居发现协议等作用域应该在本地链路的数据包限制在本地链路上，使在远程实施基于该类协议的本地链路攻击手段成为可能。但该类问题可通过配置相应的防火墙规则进行避免。ASA5505 默认情况下对逐跳选项扩展报头和目标选项扩展报头没有限制，也不能通过对防火墙的配置进行限制。该问题可能导致 DoS 攻击和规避防火墙通信内容检查的隐蔽通信。

由于 IPv6 协议中，一个数据包可携带的扩展报头数量没有限制，导致防火墙若对其逐一进行检查可能会遭受 DoS 攻击。RFC8200 和 RFC4942 建议对扩展报头及其选项进行限制，使防火墙能对扩展报头实施检查，但这也降低了 IPv6 协议原有的灵活性与扩展性。如何平衡这两者，提出新的机制是下一步研究的方向。对于路由扩展报头，如何避免被用于 DoS 攻击也是下一步研究的重点。

参考文献：

[1] NRO. Free pool of IPv4 address space depleted [EB/OL]. (2011-02-03) [2018-01-21]. https://www. nro. net/ipv4-free-pool-depleted/.

[2] APNIC. IPv4 address allocation report [EB/OL]. (2018-03-06) [2018-03-06]. https://labs. apnic. net/ipv4/report. html

[3] Goldsmith D, Schiffman M. Firewalking [Z]. Cambridge: Technology Partners Enterprise Security Services. 1998.

[4] 刘福超. 基于 HTTP 隧道的个人防火墙穿透技术研究 [D]. 上海: 上海交通大学, 2010.

[5] Davies E, Mohacsi J. RFC 4890, Recommendations for filtering ICMPv6 messages in firewalls [S]. 2007.

[6] Huitema C. RFC 4380, Teredo: tunneling IPv6 over UDP through network address translations (NATs) [S]. 2006.

[7] Abley J, Savola P, Neville-Neil G. RFC 5095, Deprecation of type 0 routing headers in IPv6 [S]. 2007.

[8] Perkins C, Johnson D, Arkko J. RFC 6275, Mobility support in IPv6 [S]. 2011.

[9] Davies E, Savola P. RFC 4942, IPv6 transition//coexistence security considerations [S]. 2007.

[10] Gont F, Linkova J, Chown T, *et al.* RFC 7872, Observations on the dropping of packets with IPv6 extension headers in the real world [S]. 2016.

[11] Gont F, Liu W, Bonica R. Recommendations on the filtering of IPv6 packets containing IPv6 extension headers [EB/OL]. (2017-10-30) [2018-01-21]. https://tools. ietf. org/html/draft-ietf-opsec-ipv6-eh-filtering-04.

[12] Deering S, Hinden R. RFC 8200, Internet protocol, version 6 (IPv6) specification [S]. 2017.

[13] Atlasis A. Attacking IPv6 implementation using fragmentation [EB/OL]. (2012) [2018-01-21]. http://media. blackhat. com/bh-eu-12/Atlasis/bh-eu-12-Atlasis-Attacking_IPv6-WP. pdf.

[14] Goel J N, Mehtre B M. Dynamic IPv6 activation based defense for IPv6 router advertisement flooding (DoS) attack [C]// Proc of IEEE International Conference on Computational Intelligence and Computing Research. Madurai: IEEE Press, 2015: 1-5.

[15] Elejla O E, Anbar M, Belaton B. ICMPv6-based DoS and DDoS attacks and defense mechanisms: review [J]. IETE Technical Review, 2017, 34 (4): 1-18.

[16] Debbarma S, Debnath P. Internet protocol version 6 (IPv6) extension headers: issues, challenges and mitigation [C]// Proc of International Conference on Computing for Sustainable Global Development. New Delhi: IEEE Press, 2015: 923-928.

[17] Hendriks L, Velan P, Schmidt R D O, *et al.* Threats and surprises behind IPv6 extension headers [C]// Proc of Network Traffic Measurement and Analysis Conference. Dublin: IEEE Press, 2017: 1-9.

[18] Gont F, Chown T. RFC 7707, Network reconnaissance in IPv6 networks [S]. 2016.